UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,174	01/21/2004	Akashi Satoh	JP920020242US1	4993

7590 04/29/2008

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
MAI, TAN V	

ART UNIT	PAPER NUMBER
2193	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/762,174
Filing Date: January 21, 2004
Appellant(s): SATOH ET AL.

William E. Lewis
For Appellants

EXAMINER'S ANSWER

This is in response to the appeal brief filed 01/31/08 appealing from the Office action mailed 09/26/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

This appeal involves claims 1-3 and 5-13.

After review Appellants' argument, Claim 4 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is

correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,847,981	KELLEY ET AL.	12-1998

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

Claims 1 and 3 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Kelley et al.

As per independent claim 1, Kelley et al teach, e.g., see Figs. 3-8, the claimed combination. The circuit comprises "…reduction tree" (element 524 of Fig. 3), sum register (530) and (carry register (535) and adder (560). Also, see col. 1, line 63 to col. 2, line 44 [for Wallace tree], and col. 6 line 45 to col. 7, line 9, especially lines 45-54, i.e., "accumulated sum" and "accumulated carry" for the claimed "sum calculation block" and "carry calculation block", respectively.

As per dependent claim 3, Kelley et al teach the detail features.

Claim Rejections - 35 USC § 103

Claims 2 and 5-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kelley et al.

Kelley et al have been discussed above.

As per dependent claim 2, the claim adds the "sum calculation block … multiplication over an extension field of two". The Wallace tree technique, i.e., carry save adder, is well known the Galois field and finite field, e.g., see Hansen et al (Ref. B). Kelley et al's sum output is available. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to design the claimed invention according to Kelley et al's teachings because the circuit is a multiplication/accumulation capable of performing sum of product as claimed.

Due to the similarity of independent claim 5 to the combination of claim 2 & 3, it is rejected under a similar rationale.

As per dependent claims 6-8, the claims add the detail features which are obvious to a person having ordinary skill in the art.

As per claims 9-13, the claims recite cipher circuits having multipliers as claimed in claims 1 & 5. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to design the claimed invention according to Kelley et al's teachings because the multiplier circuit can be used in Galois field / finite field device as claimed.

(10) Response to Argument

Appellants' arguments filed 01/31/08 have been fully considered but they are not persuasive. Appellants argue that:

I. Anticipation of claims 1and 3

"[r]egarding the §102(b) rejection of claims 1, 3, and 4 based on Kelley, Appellants respectfully assert that Kelley fails to teach or suggest all of the limitations in claims 1, 3, and 4, for at least the reasons presented below….

Appellants initially note that the Examiner has failed to provide any clear explanation of the reasoning in reaching the conclusion that the claims are anticipated by the cited reference (e.g., indicating the specific portions of Kelley which the Examiner believes anticipates each limitation of the claims). With regard to independent claim 1, the Examiner simply presents key words, cites general text, and cites blocks in figures without explaining with specificity how the cited reference anticipates the claim. **And with regard to claims 3 and 4, the Examiner simply argues that Kelley teaches the claimed limitations**….

Appellants further submit that Kelley fails to anticipate the claimed limitations. More specifically, Kelley does not teach a Wallace tree block calculating partial products for two input values as objects of multiplication and adding the partial products into a redundant binary form as recited in claim 1. **Further, Kelley does not teach a carry propagation adder converting a redundant binary number outputted from the**

Wallace tree block into a resulting product in two's complement form as recited in claim 1....

Figure 4 of Kelley depicts an adder 560. However, no where does Kelley teach or suggest the adder converting a redundant binary number outputted from the Wallace tree block into a two's complement form. The only reference to "two's complement" is found at Kelley, col. 6, lines 17-22:

> [W]hen the values of a(i) or b(i), or both, have slight restrictions placed on them, such as when the a(i) or b(i), or both, are two's complement numbers, and a(i) and b(i), or both, never have a maximum negative value, the number of bits in one or both of the sum register 580 and the carry register 585 can designed to be yet one bit smaller.

Appellants respectfully contend that the Examiner has yet to cite a portion of Kelley that teaches a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a resulting product in two's complement form....

Next, Appellants respectfully submit that the Examiner's argument fails to support the anticipation rejection. Regardless of the fact that a final result of an adder may be in two's complement form if one of operand a(i) / b(i) are two's complement numbers, the Kelley reference does not teach a carry propagation adder converting a redundant binary number outputted from the Wallace tree block into a resulting product in two's complement form. Accordingly, it is believed that the teachings of Kelley fail to meet the limitations of claim 1" (emphasis **bold face**).

II. Obviousness of claims 2 and 5-13

"[w]ith regard to the §103(a) rejection of claims 2 and 5-13, Appellants initially note that a proper case of obviousness has not been presented if the references, when combined, do not teach or suggest all the claim limitations....

With regard to claim 2, **Appellants initially note that claim 2 is patentable due to its dependence from claim 1, the patentability of which was discussed above. Next, the Kelley reference, even if modified, fails to teach or suggest a result of the calculation of the sum calculation block is outputted as a result of the multiplication over an extension field of two, as recited in claim 2**. The Examiner argues in the Final Office Action at page 3, third full paragraph, that:

> "result of the multiplication over an extension field of two" is merely a result of Galois field / finite field computation. Hansen et al (Ref. B) does Wallace tree technique, i.e., carry save, adder, in the Galois field and finite field.

Although Hansen mentions a Wallace tree and Galois fields, Appellants assert that Kelley combined with Hansen fails to teach that a result of the calculation of the sum calculation block (of the Wallace tree block recited in claim 1) is outputted as a result of the multiplication over an extension field of two.

Furthermore, the Examiner presents insufficient evidence for a motivation or suggestion to combine or modify the cited references. The Examiner argues in the Final Office Action, pg. 3, third full paragraph:

> Therefore, it would be obvious to a person having ordinary skill in the art to use to sum "portion" of the 4-2 ADD (Fig. 211) as the claimed "result of the multiplication over an extension field of two."

With regard to the §103(a) rejection of claim 5, the Examiner refers to claim 5 as being similar to the combination of claims 2 and 3, and is thus rejected under a similar rationale. Appellants assert that claim 5 is patentable for at least the reasons discussed above with regard to claims 2 and 3.

With regard to claims 6-8, Appellants assert that the claims are patentable due to their dependence from claim 5, the patentability of which was discussed above. Further, in rejecting the claims, the Examiner simply states in the Office Action, page 4, paragraph six, that "the claims add the detail features which are obvious to a person having ordinary skill in the art." **Appellants disagree and request that the rejection of claims 6-8 be withdrawn because the Examiner failed to submit evidence supporting this contention**. Furthermore, Appellants respectfully submit that the Examiner's argument is another conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court.

With regard to the rejection of claims 9-13, Appellants initially submit that independent claim 9 includes limitations similar to those of claim 1, and is therefore believed allowable for reasons similar to those described above with reference to claim 1. Further, independent claim 13 includes limitations similar to those of claim 5, and is therefore believed allowable for reasons similar to those described above with reference to claim 5. Also, dependent claims 10-12 recite patentable subject matter at least by virtue of their respective dependency from independent claims 1 and 9, and also recite patentable subject matter in their own right".

In rejecting claims 9-13, the Examiner argues in the Office Action, page 4, last paragraph, that "[i]t would have been obvious to a person having ordinary skill in the art at the time the invention was made to design the claimed invention according to Kelley et al's teachings because the multiplier circuit can be used in Galois field / finite field device as claimed." Appellants respectfully submit that this is a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See KSR v. Teleflex, No. 13-1450, slip. op. at 14 (U.S., Apr. 30, 2007), ~ In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). **There has been no showing in the present § 103(a) rejection of objective evidence of record that would motivate one skilled in the art to combine Kelley with Galois fields and finite fields to produce a cipher circuit as recited in the claims**. **Appellants respectfully contend that neither Kelley nor Hansen discuss a cipher circuit. Furthermore, the Examiner fails to explain with specificity how the combined references teach or suggest <u>each and every claimed limitation</u>**" (emphasis **bold face**).

With respect to the arguments, the examiner carefully reviews Appellants' specification, drawings, claimed invention and the applied reference.

<u>I. Anticipation of claims 1 and 3</u>

It is noted that: **(1)** the terms "carry save form" and "redundant binary form" (claim 1, line 3 or 4) are interchangeable in the art, i.e., see Appellants' specification, page 7, line 10; and **(2)** the phrases "carry propagation adder converting a redundant binary number" (claim 1, line 4) and "adder (e.g., adder 740 of Fig. 3) for adding SUM and CARRY into a final result" (Kelley et al) are the same function.

Kelley et al teach ALL of the limitations in claim 1. For example, the **(1)** " multiply reduction tree" (element 524 of Fig. 3), sum register (530) & carry register (535) and **(2)** adder (560) are considered the claimed "Wallace tree block" and "carry propagating adder", respectively. Kelley et al do disclose "Wallace multiplier tree", e.g., see col. 1, line 63 to col. 2, line 44, especially col. 2, line 14. It is noted that Kelley et al's "sum calculation block" and "carry calculation block" are parts of the " multiply reduction tree" (element 524 of Fig. 3), iterations via feed back loops. The final results stored in sum register (530) & carry register (535) are the same as the claimed "a result of the calculation of the sum calculation block and a result of the calculation of the carry calculation block" (claim 3, lines 1-3), e.g., see col. 6 line 45 to col. 7, line 9, especially lines 45-54, i.e., final "accumulated sum" and final "accumulated carry" for the results of claimed "sum calculation block" and "carry calculation block", respectively.

Kelley et al teach ALL of the limitations in claim 3. The adder (560) should be a carry propagation adder for adding SUM and CARRY into a final result, i.e., see col. 3,

line 16-17 for a similar adder, "[s]ince the adder 540 [of Fig. 1] includes a carry propagation addition to reduce separate sum and carry results into a single number...".

Kelley et al teach or suggest adder (e.g., adder 740 of Fig. 3) for adding SUM and CARRY into a final result in two's complement, e.g., see col. 6, lines 17-22:

> [W]hen the values of a(i) or b(i), or both, have slight restrictions placed on them, such as when the a(i) or b(i), or both, are two's complement numbers, and a(i) and b(i), or both, never have a maximum negative value, the number of bits in one or both of the sum register 580 and the carry register 585 can designed to be yet one bit smaller.

It is clear that Kelly et al's multiply and accumulate circuit which receives the values of a(i) and / or b(i) in two's complement numbers could perform such values. Therefore, the result of the adder (e.g., adder 740 of Fig. 3) should be in two's complement numbers.

II. Obviousness of claims 2 and 5-13

It is submitted that Kelley et al do not show the claimed "sum calculation block … multiplication over an extension field of two"; however, the Wallace tree technique, i.e., carry save adder, which only uses the SUM portion is well known the Galois field and finite field, e.g., see Hansen et al (recorded reference B Pub. No. 2003/0110197, paragraph [0047]

> "[i]n order to compute polynomial or Galois products, the full adders in

> FIGS. 4 and 5 perform either the normal 3:2 carry-save addition, or by assertion of a polynomial signal, not otherwise shown in the diagram, inhibit the carry signal altogether. The inhibition of the carry signal cause the summation of the partial products to proceed in the fashion required for a polynomial multiplication. It can be noted that certain of the full adders, including all those in FIG. 5, have at least one input which comes from the carry output of another full adder, or an input that comes from a partial product which will be known to have zero value during polynomial multiplication. Such full adders can inhibit carry propagation only from the inputs which are may be non-zero during polynomial multiplication, saving a small amount of power and area of the logic").

Kelley et al's sum output portion is available. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to design the claimed invention according to Kelley et al's teachings because the circuit is a multiplication/accumulation capable of providing the sum portion of product in Galois field application as claimed.

It is submitted that Kelley et al do not show the detail of dependent claims 6-8; however, the claimed (1) "exclusive OR operation" feature and (2) "half adders" and "full adders" features are well known in the (1) adder art and (2) Wallace tree art, respectively.

It is noted that the recitation "cipher circuit" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded

any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Tan V Mai/
Primary Examiner
Art Unit 2193

Conferees:

/Lewis A. Bullock, Jr./
Supervisory Patent Examiner, Art Unit 2193

/Eddie C Lee/

Supervisory Patent Examiner, TC 2100